12 FAM 680

REMOTE ACCESS AND MOBILE COMPUTING TECHNOLOGY

(CT:DS-221; 11-13-2014)
(Office of Origin: DS/SI/CS)

12 FAM 681 PURPOSE AND APPLICABILITY

(CT:DS-221; 11-13-2014)

This chapter establishes the minimum automated information system (AIS) security standards for remote access from, and processing of Department Unclassified/Sensitive But Unclassified (SBU) information on, non-Department systems; and for secure processing of Department information on mobile devices. This chapter applies to all users remotely accessing and/or remotely processing Department Unclassified/SBU information *from non-Department systems.*

12 FAM 682 REMOTE ACCESS FROM AND PROCESSING OF DEPARTMENT UNCLASSIFIED/SBU INFORMATION ON NON-DEPARTMENT SYSTEMS

12 FAM 682.1 SCOPE

(CT:DS-221; 11-13-2014)

a. This policy establishes the minimum security requirements for remote access from, and processing of Department Unclassified/SBU information on, non-Department systems. Remote access to Department classified networks is *unauthorized*.

b. For purposes of this subchapter, “remote access” refers to accessing Department SBU and Unclassified networks, either domestically or abroad, from non-Department systems (e.g., personally-owned or public access computers, *personal digital assistants* (PDAs), laptops, multi-function cell phones) via a Department-approved remote access program. Remote access includes but is not limited to:

(1) Department e-mail, contacts, and calendars;

(2) Department major and minor applications;

(3) Intranet, Extranet, and Internet browsing;

(4) File access privileges (e.g., read, write, and execute);

(5) Remote storage and printing;

(6) Sensitive data storage (e.g., hard drives, flash memory drives, etc.).

NOTE: *Information Assurance (IRM/IA), in coordination with the Office of Computer Security (DS/SI/CS), may approve remote administration/maintenance on any Department information system from a domestic off-site location (e.g., system administrator's home). Abroad, remote administration or maintenance is prohibited from non-Department systems.*

c. "Remote processing" refers to processing Department information on non-Department systems at non-Department facilities.

d. This chapter does not apply to:

(1) Department-owned systems (e.g., Secure Dial-In (SDI) laptops, Information Technology Change *Configuration* Control Board (IT CCB)-approved Blackberry-type devices, etc.);

(2) Access to Department public Web sites via either personally-owned, public access, or other Government agency computers;

(3) Dedicated connections, such as approved tail circuits to contractors or inter-agency connectivity; or

(4) Information Resource Center (IRC) and American Service Center (ASC) *Dedicated Internet Networks* (DINs) that permit connectivity from non-Department-owned computers.

12 FAM 682.2 Policy

12 FAM 682.2-1 Remote Access Authorization

(CT:DS-221; 11-13-2014)

a. Remote access to Department networks from non-Department-owned systems (e.g., personally-owned or public access computers) is only authorized via Department-approved remote access programs. Users accessing the Department's networks under any authorized remote access program must meet the requirements stipulated in this policy as well those of the specific remote access program under which they are connecting. When the policy requirements and the program requirements differ, the more stringent *of the two* requirements will apply.

b. Personnel must use the Department's approved method for secure remote access of PII on the Department's SBU network. The computers used must meet the requirements of 12 FAM 682.2-5*.*

c. Personnel may use remote access programs in support of the Department's telecommuting program. In those instances where the telecommuter remotely accesses the Department via a non-Department-owned system, he or she must abide by these policy requirements as well as the 3 FAM 2360 and the 12 FAM 625.2-3, Telecommuting Policies.

d. Remote access is restricted to personnel who possess a Department-issued identification card or are cleared U.S. citizens (as defined in 12 FAM 090) *who* have security clearances verified by the Office of Personnel Security and Suitability (DS/SI/PSS), and have a Department network account. This includes Department*, but is not limited to,* full-time employees (FTEs), *permanent part-time employees* contractors, *Locally Employed Staff (LE Staff),* and other-agency tenant personnel.

e. In countries that have a post rated at the Critical Technical Threat or *Human Intelligence (HUMINT)* Threat level by the Department's Security Environment Threat List (SETL), use of remote access is subject to additional restrictions. Specifically, use of remote access within such countries is authorized only:

(1) For U.S. citizens who hold security clearances at the SECRET level or higher; and

(2) From U.S. Government-owned or leased facilities.

f. Remote access by other personnel or from other locations—including public access terminals or public access wireless access points—is strictly prohibited unless an exception *is* approved in writing by DS/SI/CS and IRM/IA. Such exceptions *are* approved only for emergency situations and generally will not be granted in countries with a post that has a Technical or HUMINT Threat rating of Critical.

12 FAM 682.2-2 Remote Access Management Responsibilities

(CT:DS-221; 11-13-2014)

a. Management must exercise particular care and judgment with regard to records and information that are SBU, *containing* personally identifiable information (PII), and/or are subject to specific controls under the Privacy Act. Offices allowing employees to remotely access these records must ensure that the administrative, technical, and physical safeguards stipulated in this policy are implemented and maintained to *protect* the confidentiality and integrity of *the* records.

b. A U.S. citizen direct-hire supervisor and either management officer or executive director must:

(1) Approve in writing all requests for remote access by individual users;

(2) Ensure that a sufficient business requirement exists; and

(3) Notify the user's servicing *Information System Security Officer (ISSO).*

Overseas, the regional security officer (RSO) *must review and clear all requests* *for remote access* to ensure that adequate consideration is given to the local threat environment.

c. *The ISSO must keep a list of all users with remote access. The ISSO must review this list on an annual basis to ensure* the list is current and accurate. The ISSO must also keep a copy of the supervisor's written approval for each user authorized to access or process PII.

d. Upon user departure from *the* bureau/post, the ISSO must sign the user's check-out form indicating that all Department-owned remote access devices *were* turned in and the user's remote access capabilities *were* deactivated). The ISSO must also confirm whether the user *was* authorized to access or process PII. For authorized users, the ISSO must instruct the users to remove all PII from their computer or removable media, using a file shredder application. This software will permanently delete the files without damaging the computer or media. The DS/IS/CS Home Use – File Destruction Web Page lists several available shredding products.

12 FAM 682.2-3 Configuring Remote Access Accounts

(CT:DS-221; 11-13-2014)

a. Remote Logon access must use two-factor authentication: something a user "knows" (e.g., a password/passphrase) and something a user "has" (e.g., *a* one-time password).

b. Remote access program managers (e.g., the Messaging System Office (IRM/OPS/MSO) for OpenNet must ensure that all remote access portals display the Department's pre-logon warning message on the initial logon page.

c. *Users must secure remote* access transmission links to the Department's networks, at a minimum, with National Institute of Standards of Technology (NIST) Federal Information Processing Standard (FIPS) 140-2, level 2, certified encryption products. Encryption products must be configured in accordance with the associated product security policy listed with each product in the NIST approval list. The approval list may be found on the NIST Web site under the Cryptographic Module Validation Program.

d. Remote access program managers must configure the remote OpenNet session to lock the OpenNet server after 20 minutes of inactivity. The remote access *program manager must configure the remote access program* to ensure that user re-authentication is required each time a user logs in.

e. The user's servicing ISSO, in coordination with the user's U.S. citizen direct-hire supervisor, must ensure that user access privileges reflect the separation of key duties users perform with respect to specific applications (e.g., *users must not log in to* system administrator accounts *or* database management accounts *as if they were* data entry accounts, etc.) *Remote access program managers must ensure that each user is entered into the Mobile Computing Management System prior to enabling remote access.*

f. *Abroad, remote* access is only authorized for user-level privileges; *domestically, IRM/IA and DS/SI/CS may approve* remote administration *or* maintenance.

g. *Supervisors* may direct subordinates to not process especially sensitive information on a personally-owned or public access computer. (See 12 FAM 622.1-5.)

12 FAM 682.2-4 Remote Processing Authorization

(CT:DS-221; 11-13-2014)

a. Management and employees must exercise particular care and judgment with regard to records and information that are SBU, contain PII, or are subject to specific controls under the Privacy Act. Offices allowing employees to remotely process these records must ensure that appropriate administrative, technical, and physical safeguards are maintained to protect the confidentiality and integrity of records.

b. Users must not store or process SBU or PII (other than basic personal information or contact information for colleagues and professional associates) on non-Department-owned computers unless it is necessary in the performance of their duties.

c. U.S. citizen direct hire supervisors must:

(1) Approve, in writing, users processing PII on non-Department-owned devices; and

(2) Advise the user that all storage media (e.g., hard drives, flash memory, etc.) containing SBU or PII must be encrypted with products certified by NIST FIPS 140-2.

Users must configure the encryption products in accordance with the NIST security policy provided with the certified product. A list of NIST products certified under the Cryptographic Module Validation Program may be found at NIST's Module Validation List Web page.

12 FAM 682.2-5 User Responsibilities for Remote Accessing or Processing of Department Unclassified/SBU Information

(CT:DS-221; 11-13-2014)

a. Users must adhere to the requirements set forth in 12 FAM 543, Access, Dissemination, and Release, when accessing or processing Department SBU or PII. In accordance with 12 FAM 543, users must ensure that:

(1) Discretion is exercised *when* saving SBU or PII (e.g., save only when required). Users may save SBU or PII only to media under the user's continuing control (e.g., a personally owned computer hard drive or diskette, etc.). Users may not save SBU or PII on a hard drive that is accessible to the public (e.g., an Internet café, a public library, a document

sharing site);

(2) All Department SBU or PII is encrypted as stated in 12 FAM 682.2-4 c;

(3) Discretion is exercised *when* printing SBU data (e.g., public printers will temporarily retain data images until overwritten). PII must not be printed in public locations (e.g., a kiosk, an Internet café);

(4) *Users must secure* SBU or PII stored in hard copy format or on removable media as stated in 12 FAM 544.1, FAX Transmission, Mailing, Safeguarding/Storage, and Destruction of SBU.

b. Users with individually assigned fobs must not share their remote access passwords and authentication tokens with *others*. Users with group assigned fobs (e.g., duty officers) must have individually assigned UserIDs and Passwords for OpenNet. Group UserIDs and passwords on OpenNet are prohibited. Password controls must be in accordance with 12 FAM 622.1-3.

c. While connected remotely, users must lock user-owned and managed computers (e.g., CTRL+ALT+DEL) or, if not possible, close the remote access session when the user needs to temporarily leave the workstation. If the CTRL+ALT+DEL option is used then a twenty minute screen saver lockout feature must also be enabled as a backup security measure. To use these options, *users must configure* the computer to *require* passwords. *The DS/SI/CS Home Use Web page contains information* on implementing screen savers and passwords.

d. Users must never leave a remote access session unattended at a public location. They must log out of the session and close the browser *and* remote access program before leaving the computer.

e. Upon logout from a remote access session, users must verify the logout confirmation screen *display* before leaving the workstation.

f. Users must exercise discretion when using remote access in public areas and take prudent measures (e.g., shield the screen from public view) to minimize unauthorized data viewing.

g. Users must destroy SBU and PII files *they* have saved on their personally-owned and managed computers and removable media when the files are no longer required. *Users must destroy the files* using a file shredder application to minimize file recovery. *The DS/SI/CS Home Use Web page contains information* on file shredder applications.

h. When using personally-owned computers for remote access or remote processing of Department data, users must implement basic home security controls, to include deploying a firewall, anti-spyware, antivirus, and file destruction applications. *Users must keep upgrades and* updates to these applications current. Further, *users must apply* security patches for operating systems and applications as soon as possible. *The DS/SI/CS Home Use Web page contains information* on firewall, anti-spyware, antivirus, and file destruction software.

i. In addition to the above security controls, when using wireless capabilities on a personally-owned computer, users must enable NIST certified encryption algorithms (e.g., AES, 3DES, etc.) across the wireless link as a secondary layer of security for data transmissions. *The* DS/SI/CS Home Use - Wireless Network Web page *contains further* information on configuring wireless access points. At a minimum, *users must configure* personally-owned wireless access points as follows:

   (1) Disable the Service Set Identifier (SSID) broadcast mode in the wireless network base station (e.g., router);

   (2) Change the SSID so that only those configured with the same SSID can communicate with base stations having the same SSID;

   (3) At a minimum, implement Wireless Protected Access 2 (WPA2) encryption. WPA2 uses AES encryption to secure the link; and

   (4) Change the default wireless network base station’s administrator password to a password sufficiently complex as to not be easily guessed.

j. When using personally-owned power-line networks (i.e., personally owned computers networked via home electrical outlets) users must change the default passwords on all power-line devices, and provide link encryption using NIST-certified encryption algorithms (e.g., AES, 3DES, etc.).

k. When using a networked personally-owned computer (e.g., a home network), users must ensure that all computers on the network implement the security requirements identified above in paragraphs "h", "i", and "j" (e.g., firewall, anti-spyware software, file/hard drive encryption for SBU, hard drive encryption for PII, and NIST-certified encryption for a wireless or power-line network).

12 FAM 682.2-6 Cyber Security Incidents

(CT:DS-221; 11-13-2014)

a. Users must report the (actual or suspected) loss, theft, or compromise of the following:

   (1) A Department-owned remote access device or associated Department-owned media;

   (2) Non-Department-owned media (e.g. hard drive, CD) containing SBU information; or

   (3) An access token (e.g., a smartcard) within 24 hours or the next duty day of the event, whichever comes first, to the information system security officer (ISSO), system manager*, and U.S. citizen direct hire supervisor*.

   If the device or media (Department-owned or non-Department-owned) contained PII, *the user must also immediately report the loss, theft or compromise event* to the computer incident response team (*DS/CS/MIR*).

DS/CS/MIR is available 24 hours a day, seven days a week and may be contacted via *Unclassified* e-mail at CIRT@state.gov; classified e-mail at CIRT@state.sgov.gov; or by telephone at (301) 985-8347. *DS/CS/MIR* must promptly notify the Office of Investigations (OIG/INV) when the loss, theft, or compromise of a device or media contains PII data. (*Federal mandate also requires DS/CS/MIR* to notify the U.S. Computer Emergency Readiness Team (US-CERT) within one hour of receiving the report.) *The* Bureau of Administration's PII Breach Response Policy Plan *contains more information on reporting a PII breach.*

b. In the event that an authentication "token" (e.g., the password fob or a Department Smart ID card) is reported missing, the user's servicing ISSO, bureau security officer (BSO), or primary unit security officer (PUSO), or RSO who oversees the user's account, must ensure that the user's capability to logon remotely is immediately disabled. The user's remote access privileges may be reinstated upon re-issuance of a new token. Loss of *a* Smart ID *card* must be immediately reported to the user's *Public Key Infrastructure (PKI)* representative or the Department's Certification Authority.

c. The ISSO must ensure that all cyber security incidents are reported as required in 12 FAM 590, Cyber Security Incident Program.

12 FAM 683 PERSONAL DIGITAL ASSISTANTS

12 FAM 683.1 Scope

(CT:DS-221; 11-13-2014)

a. Personal Digital Assistants (PDAs) are hand-held computers, subject to the general requirements of 12 FAM 600. This section addresses specific requirements as they apply to PDAs. *For the purposes of this policy, a PDA is a small handheld computer that can communicate with other equipment or systems using cellular, Wi-Fi, Bluetooth, or other communication methodologies that employ radio frequency transmissions. This policy does not apply to laptops, notebooks or tablets.*

b. This policy encompasses a risk-managed approach that combines the use of security technology products with user training and awareness to minimize the vulnerabilities that are inherent with using PDAs.

c. This policy does not apply to the use of PDAs in sensitive compartmented information facilities (SCIFs). Contact *the DS Special Security Operations Division (DS/IS/SSO)* for applicable guidance.

d. This policy applies to PDAs, whether issued by the Department or owned by individuals/other entities, *which* process Department Unclassified/SBU data, or *which users bring* into Department facilities.

e. Classified processing and/or classified conversation on a PDA *are* prohibited.

f. This policy supplements the AIS policies found in 12 FAM 620 and 12 FAM 640.

g. This policy does not apply to portable U.S. Government-owned inventory scanners, which are infrequently brought into areas for short periods and remain mobile in their usage.

12 FAM 683.2 Policy

12 FAM 683.2-1 General Requirements for all PDAs

(CT:DS-221; 11-13-2014)

a. Domestically*, unless otherwise provided herein, users* may *bring PDAs* into Department areas in accordance with the requirements stipulated in this policy.

b. Abroad, PDAs are not permitted in controlled access areas (CAAs) except as authorized in the Overseas Security *Policy Board (OSPB)* Standards and Handbook, 12 FAH-6 H-311.7, H-312.7, H-313.7, and H-314.7, Unclassified Electrical/Electronic Equipment, or as approved under a separate Department-approved program.

c. Depending on the multimedia/connectivity capabilities of the PDA, additional Department policies and local standards may apply. Contact ISSO and *the* BSO, PUSO, or RSO for further guidance.

d. Department managers may impose more stringent requirements for their specific work areas if the frequency, density, or nature of classified discussions/processing warrants additional restrictions. For example, external cell phone lock boxes may be required.

e. PDA users may not use PDA audio recording and/or video/still photography features in Department areas where classified information may be processed, viewed, or discussed. PDA users may use PDA audio recording and/or video/still photography features only in Department designated public areas; e.g., cafeteria. Contact *the Office of Domestic Facilities Protection (DS/DO/DFP)* for approval of domestic areas and the RSO for approval abroad.

f. When *viewing Department data* away from Department facilities, users must be aware of their environment; e.g., public spaces, and take prudent measures; e.g., shield the PDA screen from public view to minimize unauthorized data viewing.

g. PDA users are responsible for exercising due care to prevent loss, theft, or compromise of Department information and equipment.

h. Users must operate PDAs in compliance with this policy.

i. Users must disable all Bluetooth and Near Field Communication technologies within Department facilities.

12 FAM 683.2-2 Department-Owned PDAs

(CT:DS-221; 11-13-2014)

a. *Users must meet the* general policies in 12 FAM 683.2-1.

b. The Information Technology *Configuration* Control Board (IT CCB) must approve all Department-owned *Enterprise* PDAs and *those PDAs* must be part of a Department-approved program *(e.g., BlackBerrys). The IT CCB or local CCB must approve all Department-owned Non-Enterprise PDAs (e.g., iPhone, Android).*

c. The system manager must configure Department-owned PDAs in accordance with Department Security Configuration Guidelines (e.g., anti-virus software, identification and authentication controls, a time-out feature, and audit capabilities*), when available.* Additionally, *IT CCB-* or local CCB-approved firewall and file shredder applications, where available, must be installed. The *DS/SI/CS website* lists several shredding and firewall products.

d. Users must not disable or alter security features on Department-owned PDAs.

e. When available, *the system manager must install* encryption that secures the data-at-rest on all Department-owned *Unclassified*/SBU PDAs and associated media. The encryption products must be certified in accordance with the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2. *The system manager must configure the* encryption product in accordance with the NIST security policy provided with the certified product. A list of NIST products certified under the Cryptographic Module Validation Program may be found at the *NIST website.*

f. U.S. citizen direct-hire supervisors must:

(1) Approve the distribution and use of Department-owned PDAs;

(2) Confirm *that the Department-owned Enterprise* PDAs are *IT CCB-*approved and part of a Department-approved program*, or that the Department-owned Non-Enterprise PDAs are either IT CCB-approved or local CCB-approved;*

(3) Ensure that PDAs are accounted for in a property inventory;

(4) Ensure that users approved for use of a PDA *have successfully completed the PS800 Annual Cybersecurity Awareness Course;* and

(5) Ensure the PDA is labeled with instructions on whom to contact if found.

g. Any PII stored or processed on the PDA must be only the minimum amount reasonably necessary to accomplish the user's work and should be immediately deleted when no longer needed.

h. Only Department-owned Enterprise PDAs that are IT CCB-approved, part of a Department-approved program, and configured in accordance with Department Security Configuration Guidelines, may connect/synchronize with a Department network, e.g., OpenNet, as allowed for under the Department-approved program. Wireless connectivity to a Department network must be secured using NIST FIPS 140-2 certified encryption. The encryption product must be configured in accordance with the NIST security policy provided with the certified product.

i. Department-owned PDA users must report (actual or suspected) PDA or associated media loss, theft, or compromise within 24 hours or the next duty day after the event, whichever comes first, to the *ISSO,* system manager, and *U.S. citizen direct hire supervisor*. If the PDA or associated media contained PII, the event must also immediately be reported to DS/CS/MIR. *Users may contact* DS/CS/MIR 24 hours a day seven days a week via *Unclassified* email at CIRT@state.gov; classified email at CIRT@state.sgov.gov; or by telephone at (301) 985-8347. DS/CS/MIR must promptly notify OIG/INV when the lost, stolen, or compromised device or media contains PII. (NOTE*: Federal mandate also requires DS/CS/MIR* to notify the U.S. Computer Emergency Readiness Team (US-CERT) within one hour of receiving the report.) *The Privacy Division (A/GIS/IPS/PRV) website contains more* information on reporting a PII breach.

j. Following the loss, theft, or compromise of a Department-owned PDA or associated media, the ISSO must ensure that the user completes a PDA refresher briefing and signs a new acknowledgement form before being issued another PDA. The U.S. citizen direct-hire supervisor must sign off that the user has completed the refresher briefing. The user must also notify their bureau's Accountable Property Officer (APO) for proper inventory adjustment.

k. Domestically, *users must dispose of* Department-owned *Unclassified*/SBU PDAs and all associated media in accordance with 12 FAM 629.2-4, Sensitive Media, Output, and Equipment Disposition. Abroad*, users must dispose of* Department-owned *Unclassified*/SBU PDAs in accordance with 12 FAH-6 H-542.5-10, Disposal/Disposition.

l. *Users must return* Department-owned PDAs to the ISSO, system manager, or *U.S. direct hire supervisor* when no longer required.

m. Upon permanent departure from bureau/post, users must indicate on their check-out form whether or not they had a Department-owned PDA and, if yes, that they have returned it to the *ISSO,* system manager, or *U.S. direct hire supervisor.*

12 FAM 683.2-3 Non-Department-owned PDAs

(CT:DS-221; 11-13-2014)

a. Non-Department-owned PDAs include personally-owned, vendor-owned, contractor-owned, and *other* U.S. Government agency-owned PDAs.

b. All Department employees are responsible for ensuring that their visitors are aware of, and comply with these policies.

c. Domestically, *Department managers may allow* non-Department-owned PDAs *within their specific work areas provided users maintain a minimum of 10 foot (3 meter) separation between the PDA and classified processing equipment.* Additionally, PDAs equipped with a camera in these areas must have the camera lens covered at all times; e.g., placed inside a briefcase, a purse, or a holster if it covers the lens, etc.

d. Abroad, non-Department-owned PDAs are prohibited in CAA spaces.

e. Non-Department-owned PDAs *must* not connect with a Department network except via *the* Department-approved remote access *method.*

f. Personnel must use the Department's approved method for secure remote access of PII on the Department’s SBU network. The computers used must meet the requirements of 12 FAM 682.2-5

12 FAM 684 THROUGH 689 UNASSIGNED